THE ARITHMETIC OF POLYNOMIALS IN A GALOIS FIELD

By Leonard Carlitz*

Department of Mathematics, California Institute of Technology

Communicated December 30, 1930

1. Let p be any prime (including 2) and π any positive integer; let $GF(p^\pi)$ be the Galois field of order p^π. We define[1] $\mathfrak{D}(p^\pi, x)$ as the totality of polynomials in an indeterminate, x, with coefficients in the $GF(p^\pi)$. In this paper we consider some of the arithmetic properties of the polynomials in $\mathfrak{D}$.

2. If M is a polynomial in $\mathfrak{D}$, $sgn\ M$ is the coefficient of the highest power of x; if $sgnM = 1$, M is primary. If M is of degree μ, $|M|$ by definition $= p^{\pi\mu}$. Now the number of primary polynomials of degree μ is $p^{\pi\mu}$. Accordingly we define the ζ-function in $\mathfrak{D}$ by

$$\zeta(s) = \sum_F \frac{1}{|F|^s} = \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1} \qquad (s > 1),$$

F running over all primary polynomials, P over all primary irreducible polynomials. It is easily verified that

$$\zeta(s) = \frac{1}{1 - p^{\pi(1-s)}}.$$

3. We now define a number of numerical functions of a primary argument F (except (*vi*) which is of a different nature)

$$\mu(1) = 1,\ \mu(F) = 0 \text{ for } P^2 | F, \qquad \text{(i)}$$

$$\mu(F) = (-1)^\rho, \text{ for } F = P_1 \ldots P_\rho,$$

P_i irreducible and distinct.

$$\lambda(1) = 1, \qquad \text{(ii)}$$

$$\lambda(F) = (-1)^{\alpha_1 + \cdots + \alpha_\rho} \text{ for } F = P_1^{\alpha_1} \ldots P_\rho^{\alpha_\rho}$$

$\tau(F)$ is the number of primary divisors of F (iii)

$\sigma(F)$ is the sum of the absolute values of the primary divisors of F: (iv)

$$\sigma(F) = \sum_{D|F} |D|$$

$\varphi(F)$ is the number of polynomials of degree less than F that are prime to F. (v)

$Q(\nu)$ is the number of primary polynomials of degree ν that are not divisible by the square of an irreducible polynomial. (vi)

4. By making use of the connection between these functions and $\zeta(s)$ we deduce the following results very easily.

$$\sum_{\deg F=\nu} \mu(F) = 0 \quad \text{for } \nu \geqq 2, \tag{i}$$

$$\sum_{\deg F=1} \mu(F) = -p^{\pi}$$

$$\sum_{\deg F=\nu} \lambda(F) = (-1)^{\nu} p^{\pi[(\nu+1)/2]}, \tag{ii}$$

where $[\alpha]$ is the greatest integer $\leqq \alpha$.

$$\sum_{\deg F=\nu} \tau(F) = (\nu+1)p^{\pi\nu}. \tag{iii}$$

$$\sum_{\deg F=\nu} \sigma(F) = p^{\pi\nu} \frac{p^{\pi(\nu+1)} - 1}{p^{\pi} - 1}. \tag{iv}$$

$$\sum_{\deg F=\nu} \varphi(F) = p^{2\pi\nu} - p^{\pi(2\nu-1)}. \tag{v}$$

$$Q(\nu) = p^{\pi\nu} - p^{\pi(\nu-1)} \quad \text{for } \nu > 1, \tag{vi}$$

$$Q(1) = p^{\pi}$$

These formulas are the analogs of well-known asymptotic formulas in the rational field.

5. We now give a theorem of reciprocity of index $p^{\pi} - 1$. Define $\{A/P\}$ as that element of $GF(p^{\pi})$ such that

$$\left\{\frac{A}{P}\right\} \equiv A^{(|P|-1)/(p^{\pi}-1)}, \ mod\ P, \quad P \text{ not dividing } A.$$

Then if P and Q are primary and prime to each other

$$\left\{\frac{Q}{P}\right\} = (-1)^{\rho\nu}\left\{\frac{P}{Q}\right\}, \tag{1}$$

ρ,ν being the degrees of Q, P, respectively.

From this Dedekind's theorem of quadratic reciprocity[1] follows as a special case.

6. The proof of (1) depends on three lemmas. Define $R(A/P)$ as the remainder in the division of A by P.

Lemma 1. (*Analog of Gauss' Lemma.*) *If H run through the primary polynomials of degree $<\nu$,*

$$\left\{\frac{A}{P}\right\} = \prod_{H} sgn\, R\left(\frac{AH}{P}\right).$$

Lemma 2. *If A is primary of degree $\alpha \geqq \nu$, and is not a multiple of P,*

$$sgn\, \Pi(A - KP) = (-1)^{\alpha - \nu}\, sgn\, R\left(\frac{A}{P}\right),$$

the product extending over all primary K of degree $\alpha - \nu$.

Lemma 3. *If H runs through the primary polynomials of degree* $<\nu$,

$$sgn \prod_{H,K} (HQ - KP) = (-1)^{\rho\nu + Min.\,(\rho^2,\, \nu^2)}\, sgn \prod_{H} R\left(\frac{HQ}{P}\right).$$

7. A paper containing a detailed account of the above results, as well as a number of generalizations, has been offered to the *American Journal of Mathematics*.

* NATIONAL RESEARCH FELLOW.

[1] Cf. Dedekind, R., *J. für. Math.*, **54** (1857), pp. 1–26.

THE COLORING OF GRAPHS[1]

By HASSLER WHITNEY

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY

Communicated January 14, 1931

1. *Introduction.*—We shall give here an outline of a study of the numbers m_{ij} appearing in a formula for the number of ways of coloring a graph. The details will be given in several papers. The definitions and results in a paper on Non-separable and Planar Graphs will be made use of.

2. *The Number of Ways of Coloring a Graph.*—Suppose we assign to each vertex of a graph a color in such a way that each pair of vertices joined by an arc are of different colors. (A graph containing a 1-circuit cannot be colored therefore.) We obtain thereby a permissible coloring of the graph. Given a graph G, let m_{ij} be the number of subgraphs of rank i and nullity j. Then the number of ways of coloring G in λ colors is

$$P(\lambda) = \sum_i \lambda^{v-i} \sum_j (-1)^{i+j} m_{ij} = \sum_i m_i \lambda^{v-i},$$

if G contains v vertices. This result, first found by Birkhoff,[2] is proved by a simple logical expansion.[3]

We note that, if G contains E arcs,

$$m_{i0} + m_{i-1,\,1} + \ldots + m'_{0i} = \binom{E}{i}.$$

Let G' be formed from G by dropping out the arc ab. Let $m'_{ij}(a \times b)$ be the number of subgraphs of rank i, nullity j, of G' in which a and b are in different connected pieces. Put